Testimony of Sally Katzen

before
The Committee on the Judiciary
Subcommittee on Commercial and Administrative Law

on
May 17, 2006

on
"Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security and the Privacy Officer of the Department of Justice"

Mr. Chairman and other Members of the Committee. Thank you for inviting me to testify today on a subject – "Privacy in the Hands of the Government" -- that is exceedingly important to the American public and on which this Committee has commendably been actively engaged.

This hearing is a follow on to one at which I testified on February 10, 2004. With the permission of the Committee, I would request that the written testimony that I prepared then be appended to my submission for this hearing; much of the background and analysis presented in that document remain pertinent today and incorporating it by reference will enable me to better focus on more recent developments.

I have been involved in privacy policy and practices for well over a decade, having served as the Administrator of the Office of Information and Regulatory Affairs (OIRA) in the Office of Management and Budget (OMB) from 1993 to 1998 and as the Chair of the Information Policy Committee of the National Information Infrastructure Task Force, which produced, among other things, a revision of the 1973 Code of Fair Information Practices, entitled "Principles for Providing and Using Personal Information." During my later tenure as Deputy Director of the National Economic Council and then as Deputy Director for Management at OMB, I was involved in a series of privacy issues, any my interest in the subject has continued during my years in academics.

My earlier testimony spoke to the importance of privacy in our history and culture, and why I believe that privacy is one of the hallmarks of America -- cherished, protected and defended throughout our country and throughout the years. The arrival of the Information Age raised privacy concerns to a new level, although after September 11, 2001, this was tempered by a clear recognition of the importance of security and the need for combating terrorism. But protecting our privacy and protecting our nation are not mutually exclusive goals. Rather, the challenge for all of us is to protect and defend our country in a way that preserves and promotes our core values.

I belabor this point because in the two years since I appeared before this Committee, the concern for privacy (and what many Americans believe to be invasions of their privacy) has increased rather than decreased. More articles about privacy policies and practices appear more frequently in the press, there are more stories on the radio and television, and there is significantly more attention paid to privacy on the Internet than ever before. The time devoted over the last several weeks/months in public discourse to the warrantless wiretaps by the National Security Agency and the decision of some common carriers to release to the government information about calls made by millions of Americans is a clear indication of Americans' continued commitment to, and concern about, privacy.

Given the importance of privacy and its persistence in the national debate, it is somewhat surprising that this Administration has seemed to be so reluctant to take even minimal steps to address these concerns. For example, when I last testified, I spoke of the generally highly favorable reactions to the tenure of Nuala O'Connor Kelly as the first statutorily required privacy official at the Department of Homeland Security (DHS). I stressed both the beneficial attention that was paid to privacy concerns and the fact that having a privacy officer at DHS in no way diminished the capacity of the Department to pursue its mission. Ms. Kelly resigned from DHS many months ago, and regrettably there is only an Acting privacy officer in place. Is it a lack of interest or a lack of support for the position by the current Secretary of DHS? Or by the White House? There may well be legitimate problems in finding and installing Ms. Kelly's replacement, but the unexplained delay sends a very bad signal to those who follow these developments as an indication of the Administration's commitment to privacy. In that same vein, it is worth noting that it took the longest time for the White House to nominate and have the Senate confirm the members of the Privacy and Civil Liberties Board, which is a committee established by another act of Congress designed to respond to what were perceived as legitimate questions and concerns about government policies with respect to privacy.

In light of these examples, I would call for more oversight by the Congress and, equally important, more legislation creating and empowering officials in the government with responsibility for privacy policy. I had urged in my earlier testimony that the Committee consider expanding the number of statutory privacy offices from one to 24, covering all major Departments (the so-called Chief Financial Officers Act agencies) or at least a handful of critical agencies, including the Department of Justice, the Department of the Treasury (and the Internal Revenue Service), the Department of Defense and the Veterans Administration, the Social Security Administration, and the Department of Health and Human Services. I was pleased when Congress enacted legislation establishing a privacy officer at the Department of Justice. With respect, I would again urge this Committee to work with others in the Congress to expand on this base. OMB guidance from two administrations (issued first during the Clinton Administration and repeated several years ago by the Bush Administration) has called for the creation of such offices in Executive Branch agencies. The imprimatur of Congress would enhance the influence and respect that these officers have within their Departments. Equally important, by establishing statutory privacy offices, the Congress

would be able to engage in systematic oversight of the attention paid to this important value in the federal government.

I would also renew my suggestion that Congress establish at OMB a statutory office headed by a Chief Counselor for Privacy. Such an office was created and staffed during the Clinton Administration, and it served us well. The current Administration chose not to fill the position when they took office or since. As a result, there is no senior official in the Executive Office of the President who has "privacy" in his/her title or who is charged with oversight of federal privacy practices, monitoring of interagency processes where privacy is implicated, or developing national privacy polices. Yet it is so much better to have privacy implications considered beforehand -- in the formulation of program or projects – rather than after the plans are implemented and the stories about them begin to appear on the front pages of the national newspapers. And apart from damage control, having someone on the "inside" addressing these issues may provide some brakes on the runaway train of surveillance.

Finally, I understand that after this hearing, the Committee will move to mark up H.R. 2840, the "Federal Agency Protection of Privacy Act of 2005." That bill reflects a commendable desire to ensure that privacy impact statements are prepared by federal agencies as they develop regulations that involve the collection of personal information. Several thoughts occurred to me as I was rereading the text for today's hearing.

First, Subsection (c) provides that an agency head may waive the requirements for a privacy impact statement "for national security reasons, or to protect from disclosure classified information, confidential commercial information, or information the disclosure of which may adversely affect a law enforcement effort . . ." Apart from the fact that the basis for a waiver goes well beyond national security, I recalled that there is a similar provision in the E-Government Act of 2002, which requires a privacy impact assessment for new federal government computer systems, but instead of giving an essentially free pass for national security concerns, Section 208 (b) (1) (D) of that Act requires the agency to provide the privacy impact assessment to the Director of OMB. I would recommend that such a provision be included in H.R. 2840 and, in addition, that the bill provide that a copy of the analysis be sent to the Congressional Intelligence Committees in the case of national security waivers and the Congressional Judiciary Committees in the case of law enforcement related waivers. In that way, there could be government-wide Executive Branch oversight and, equally important, Congressional oversight over agency decision-making in this area..

Second, the provisions of H.R. 2840 requiring an agency to prepare a plan for, and carry out, a periodic review of existing regulations that have a significant privacy impact on individuals or a privacy impact on a significant number of individuals are quire detailed and quite prescriptive. Rather than specifying all of the factors to be considered, and the timetable and procedures for each element of the review, it might be preferable to set forth un the bill the objectives of a periodic review and task OMB with providing guidance for the agencies as to how they should proceed. In this way, the terms are not

cast in concrete but can be more readily adjusted as changes occur, either with respect to content or with respect to technology.

With those modest suggestions, I would endorse the bill and once again commend this Committee for its effective and persistent leadership on these very important issues.

Again, thank you for inviting me to testify today. I would be pleased to elaborate on these comments or answer any questions that you may have.

APPENDIX

Testimony of Sally Katzen
before
The Committee on the Judiciary
Subcommittee on Commercial and Administrative Law
on
February 10, 2004
on
"Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security"

Thank you for inviting me to testify today on a vitally important subject – "Privacy in the Hands of the Government." This Committee is to be congratulated, not only for its leadership in creating a statutory Privacy Officer in the Department of Homeland Security (DHS), but also for being vigilant in its oversight of that office.

I am currently a Visiting Professor at the University of Michigan Law School, where one of my courses is a seminar on "Technology Policy in the Information Age" – a significant portion of which is devoted to examining both the government and the private sector's privacy policies and practices. I have been involved in privacy policy for over a decade. In early 1993, I began serving as the Administrator of the Office of Information and Regulatory Affairs (OIRA) in the Office of Management and Budget (OMB); the "I" in OIRA signaled that I was, in effect, the chief information policy official for the federal government. Among other responsibilities, my office was charged with developing federal privacy policies, including implementation of the 1974 Privacy Act. Later in 1993, I was asked to chair the Information Policy Committee of the National Information Infrastructure Task Force, which had been convened by the Vice President and chaired by then Secretary of Commerce Ronald Brown. One of the first deliverables we produced was from my committee's Privacy Working Group – a revision of the 1973 Code of Fair Information Practices, entitled "Principles for Providing and Using Personal Information." During President Clinton's second term, I worked with the Vice President's Domestic Policy Advisor to create a highly visible and effective office for privacy advocacy in OMB; we selected Peter Swire to head that office and be the first Chief Counselor for Privacy, and I worked closely with him when I served as Deputy Director for Management at OMB during the last two years of the Clinton Administration. Since leaving government, I have, as indicated earlier, been teaching both at the graduate and undergraduate level.

Given the Committee's extensive work in this area, it is not necessary to speak at length on the importance of privacy in the history and culture of our country. Nonetheless, to provide context for the comments that follow, I want to be clear that, from my perspective, privacy is one of the core values of what we are as Americans. Whether you trace its roots from the first settlers and the "frontier" mentality of the early

pioneers, or from the legal doctrines that flowed from Justice Brandeis' oft-quoted recognition in the late 19th century of "the right to be let alone," privacy has been one of the hallmarks of America -- cherished, prized, protected and defended throughout our country and throughout our history.

The "Information Age" has brought new opportunities to benefit from the free flow of information, but at the same time it has also raised privacy concerns to a new level. Computers and networks can assemble, organize and analyze data from disparate sources at a speed (and with an accuracy) that was unimaginable only a few decades ago. And as the capacity – of both the government and the private sector – to obtain and mine data has increased, Americans have felt more threatened – indeed, alarmed – at the potential for invasion (and exploitation) of their privacy.

Before September 11, 2001, privacy concerns polled off the charts. Since then, there has been a recognition of the importance of security and the need for combating terrorism. But, as the Pew Internet surveys (and others) have found, Americans' commitment to privacy has not diminished, and some would argue (with much force) that if, in protecting our nation, we are not able to preserve a free and open society for our public lives, with commensurate respect for the privacy of our private lives, then the terrorists will have won. For that reason, it was both necessary and desirable in creating a Department of Homeland Security to statutorily require the Secretary to appoint a senior official with primary responsibility for privacy policy. Ms. Kelly was selected for that position and took office about six months ago.

We thus have some – albeit limited – operational experience with the statutory scheme, and it is therefore timely to see what we have learned and what more could (and should) be done by this Committee to be responsive to privacy concerns.

I would draw two lessons from Ms. Kelly's tenure to date at DHS.

First, the existence of a Privacy Officer at DHS, especially someone who comes to the position with extensive knowledge of the issues and practical experience with the federal government, is highly beneficial. We know that some attention is now being paid to privacy concerns and that steps are being taken to advance this important value that might otherwise not have occurred.

Consider the CAPPS II project, in which Ms. Kelly has recently been involved. She inherited a Privacy Act Notice issued last winter that was dreadful. She produced a Second Privacy Act Notice that reflected much more careful thought about citizens' rights and provided more transparency about the process. Regrettably, there was some backsliding: the initial concept was that the information would be used only to combat terrorism, whereas the second Notice indicated that the information would be used not only for terrorism but also for any violation of criminal or immigration law. Also, the document was vague (at best) on an individual's ability to access the data and to have corrections made. And there was more that should have been said about the manner in

which the information is processed through the various data bases. But there is no question that the Second Notice was greatly improved from the first.

Ms. Kelly was also involved with the US VISIT program, where she produced a Privacy Impact Analysis (PIA). Some had argued that a PIA was not required because the program did not directly affect American citizens or permanent residents. Nonetheless, to her credit, she prepared and issued a PIA that was quite thoughtful and was well received. Whether one agrees or disagrees with the underlying program, at least we know that someone was engaged in the issues that deserve attention and the product of that effort was released to the public.

As someone outside the government, it is hard to know how influential Ms. Kelly will be if – and it inevitably will happen – there is a direct conflict between what a program office within DHS wants to do and what the Privacy Officer would counsel against for privacy reasons. Effectiveness in this type of position depends on autonomy and authority – that is, on the aggressiveness of the office holder to call attention to potential problems and on support from the top. We may take some comfort from Secretary Ridge's comments; he has said all the right things about supporting the Privacy Officer. But we cannot now know what will happen when the "rubber meets the road."

This Committee, however, can further empower the Privacy Officer, and lay the foundation for remedying any problems that may arise, by maintaining its oversight and inquiring pointedly into how the Department operates. For example, Ms. Kelly (and Secretary Ridge) should be asked at what stage she is alerted to or brought into new initiatives; what avenues are open for her to raise any questions or concerns; and whether the Secretary will be personally involved in resolving any dispute in which she is involved. The timing of the release of the PIA for the US VISIT program suggests that Ms. Kelly may not always be consulted on a timely basis. As I read the E-Government Act of 2002, an agency is to issue a PIA <u>before it develops or procures</u> information technology that collects, maintains or disseminates information that is in an identifiable form. In this instance, the PIA was released much further down the road, when the program was about to go on line. Anything that helps the Privacy Officer become involved in new initiatives at the outset, before there is substantial staff (let alone money) invested in a project, would be highly salutary.

The second lesson that I take from the experience to date with the Privacy Officer at DHS is that there has been no diminution in the capacity of the Department to pursue its mission. Or as a political wag would say, the existence of a Privacy Officer in DHS has not caused the collapse of western civilization as we know it. This is wholly consistent with what most Americans think – that national security and privacy <u>are</u> compatible and are not intrinsically mutually exclusive.

The fact that there is no evidence that the existence, or any activity, of the Privacy Officer has caused DHS to falter leads me to suggest that the Committee consider expanding the number of statutory privacy offices from one to 24, covering all major Departments (the so-called Chief Financial Officers Act agencies) or at least a handful of

critical agencies. Imagine the salutary effect that a statutory privacy office could have at the Department of Justice, the Department of the Treasury (and the Internal Revenue Service), the Department of Defense and the Veterans Administration, the Social Security Administration, and the Department of Health and Human Services. All of these agencies already have some form of privacy office in place, although many simply process Privacy Act complaints, requests, notices, etc. and do not involve themselves in the privacy implications of activities undertaken by their agencies. It is significant, I believe, that OMB guidance from two administrations (issued first during the Clinton Administration and repeated recently by the Bush Administration) has called for the creation of such offices in Executive Branch agencies. With the imprimatur of Congress, these offices can achieve the status (and increased influence) and gain the respect that the Privacy Officer has enjoyed at DHS. Equally important, by establishing statutory privacy offices, the Congress will be able to engage in systematic oversight of the attention paid to this important value in the federal government – something which has not occurred before this hearing today.

I hope I do not seem presumptuous to suggest – indeed, strongly urge – one further step: establishing at OMB a statutory office headed by a Chief Counselor for Privacy. As noted above, we had created such a position during the Clinton Administration, and it served us well. Peter Swire, the person we selected to head that office, was able to bring his knowledge, insights, and sensitivity to privacy concerns to a wide range of subjects. In his two years as Chief Counselor, he worked on a number of difficult issues, including privacy policies (and the role of cookies) on government websites, encryption, medical records privacy regulations, use and abuse of social security numbers, and genetic discrimination in federal hiring and promotion decisions, to name just some of the subjects that came from various federal agencies. He was also instrumental in helping us formulate national privacy policies that arose in connection with such matters as the financial modernization bill, proposed legislation to regulate internet privacy, and the European Union's Data Protection Directive.

I believe it is unfortunate that the current Administration has chosen not to fill that position. As a result, there is no senior official in the Executive Office of the President who has "privacy" in his/her title or who is charged with oversight of federal privacy practices, monitoring of interagency processes where privacy is implicated, or developing national privacy polices. Perhaps it was the absence of such a person that led to the Bush Administration's initial lack of support for the designation of a Privacy Officer at the Department of Homeland Security. Perhaps if someone had been appointed to that position, the Administration would not have appeared to be so tone deaf to privacy concerns in connection with the Patriot Act or any number of law enforcement issues that have made headlines over the past several years. An "insider" can provide both institutional memory and sensitivity to counterbalance the unfortunate tendency of some within the government to surveil first and think later. At the least, the appointment of a highly qualified privacy guru at OMB would mean that someone in a senior position, with visibility, would be thinking about these issues before – rather than after – policies are announced.

Finally, I understand that after this Hearing, the Committee will move to mark up H.R. 338, "The Defense of Privacy Act." That bill reflects a commendable desire to ensure that privacy impact statements are prepared by federal agencies as they develop regulations which may have a significant privacy impact on an individual or have a privacy impact on a substantial number of individuals. I was struck in reviewing the E-Government Act of 2002 for this testimony that it requires an agency to prepare a PIA not only before it develops or procures information technology that implicates privacy concerns, but also before the agency initiates a new collection of information that will use information technology to collect, maintain or disseminate any information in an identifiable form. This law has gone into effect, OMB has already issued guidance on how to prepare the requisite PIAs, and the agencies are learning how to prepare these PIAs using that model. Rather than impose another regime on agencies when they are developing regulations (which are frequently the basis for the information collection requests referenced in the E-Government Act of 2002), it might be preferable to amend the E-Government Act to expand its requirements to apply to regulations that implicate privacy concerns. That approach would have the added benefit of eliminating the inevitable debate over the judicial review provisions of H.R. 338, which go significantly beyond the judicial review provisions of any of the comparable acts (e.g., Reg.Flex., NEPA, Unfunded Mandates, etc.). Lastly, if you were to amend the E-Government Act to include privacy-related regulations, you might also consider including privacy-related legislative proposals from the Administration. As you know, Executive Branch proposals for legislation are reviewed by OMB before they are submitted to the Congress. If there were a Chief Counselor for Privacy at OMB, s/he would be able to provide input for the benefit of the Administration, the Congress and the American people.

Again, thank you for inviting me to testify today. This Committee has been an effective leader on privacy issues, and it is encouraging that you are continuing the effort. I would be pleased to elaborate on these comments or answer any questions that you may have.